Claims:

This listing of the claims will replace all prior versions and listings of claims in the application:

1. (Currently amended) In a computer environment that includes a document service cluster having a private key database, the document service cluster having secure access to a database of signature ready documents, the computer environment further including a plurality of remote computers coupled to the document service cluster over a computer network, a ~~A~~ method for issuing requests from the remote computers to the document service cluster for ~~of~~ signing ~~and authenticating~~ electronic documents, and signing electronic documents using the document service cluster, the method comprising:

registering each of a plurality of users using a registration process associated with the document service cluster, wherein the registration process includes:

providing, by each user, identifying information corresponding to an identity of the user;

performing a database check of the identifying information provided by each user by comparing the identifying information provided by each user against database records; and

providing a user with service credentials for accessing the document service cluster if an outcome of the database check for the user is successful, whereby the user becomes a registered user;

securely storing a plurality of private key portions associated with the ~~a~~ plurality of registered users in ~~a~~ the private key database on ~~a local~~ the document service ~~computer~~ cluster;

receiving at the ~~local~~ document service ~~computer~~ cluster a signing request and service credentials transmitted from a remote computer by a first registered user, said signing request generated in the absence of a pre-installed add-in software program configured to providing a signed message at the remote computer; wherein the service credentials received from the first registered user are independent of the remote computer used to transmit the signing request to the document service cluster;

using the service credentials received at the document service cluster to identify ~~identifying~~ the signing request as one transmitted by the first registered user, and identifying, at the document service cluster, a signature ready document, from the database of a signature ready documents, to be signed at the document service cluster in accordance with a private key portion that is associated with the first registered user and stored in the private key database;

retrieving, from the private key database at the ~~local~~ document service ~~computer~~ cluster, ~~a~~ the private key portion associated with the first registered user ~~from the private key database~~;

generating, at the document service cluster, a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

retrieving at the ~~local computer~~ document service cluster the signature ready document to be signed; and

signing the signature ready document at the ~~local computer~~ document service cluster using the ~~generated~~ complete private key to produce a signed document;

wherein the private key portion remains on the document service cluster during the signing of the signature ready document, and no storage of the private key portion occurs on the remote computer after the signing of the signature ready document.

2. (Original) The method of claim 1 wherein the private key portion is a complete private key.

3. (Currently amended) The method of claim 1 wherein generating a complete private key using the retrieved private key portion includes:

receiving ~~signing identification~~ the service credentials sent from the first user at the remote computer to the ~~local computer~~ document service cluster after receiving the signing request; and

constructing a complete private key using the private key portion and the received ~~signing identification~~ service credentials.

4. (Currently amended) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the ~~local computer~~ document service cluster over the internet.

5. (Currently amended) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the ~~local computer~~ document

service cluster over the world wide web using hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer.

6. (Currently amended) The method of claim 5 wherein the retrieving at the ~~local computer~~ document service cluster the signature ready document is automatic.

7. (Original) The method of claim 5 wherein the retrieved signature ready document is a standard generalized markup language document.

8. (Currently amended) The method of claim 1 further comprising storing the signature ready document in ~~a first document~~ the database of signature ready documents.

9. (Original) The method of claim 8 further comprising prior to signing:

receiving data from the first remote computer; and modifying the retrieved signature ready document based on the received form date.

10. (Currently amended) The method of claim 8 wherein the ~~first document~~ database of signature ready documents is located on the ~~local~~ document service cluster.

11. (Currently amended) The method of claim 8 wherein the ~~first document~~ database of signature ready documents is located on a secure second remote computer.

12. (Original) The method of claim 8 further comprising storing the signed document in a second document database.

13. (Original) The method of claim 12 wherein the second database is located on a secure second computer remote computer.

14. (Currently amended) The method of claim 12 wherein the second database is located on the ~~local computer~~ document service cluster.

15. (Original) The method of claim 12 further comprising associating at least one of the signature ready documents and the signed document with a document owner.

16. (Original) The method of claim 15 further comprising notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.

17. (Currently amended) The method of claim 1 ~~further comprising registering individual as users~~ wherein said registering includes:

verifying and recoding the identify of individuals registering;

digitizing and recording handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded

~~identifies~~ identities in an ~~identify~~ identity database, the ~~identify~~ identity database being accessible to the ~~local computer~~ document service cluster.

18. (Previously Presented) The method of claim 17 further comprising:

recording at least one biometric measurement other than a handwritten signature of individuals registering;

associating the at least one biometric measurement of individuals registering with the recorded identities of the individuals registering; and

storing the biometric measurements in the identity database.

19. (Original) The method of claim 18 further comprising detecting using the biometric measurements whether individuals previously registered.

20. (Cancelled).

21. (Currently amended) The method of claim 17 ~~20~~ wherein the signing comprises:

a) appending the first user's digitized handwritten signature to the signature ready document;

b) making a hash of the signature ready document; and

c) encrypting the hash of the signature ready document with the first user's private key.

22. (Currently amended) The method of claim 17 further comprising:

associating and storing a secret set of recognition graphics with the passwords in the identity database;

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer;

requesting the first user to select graphics including in the secret set using a non-keyboard selecting device attached to the first remote computer;

receiving a message from the first remote computer identifying the selected graphics;

authorizing access to the ~~local computer~~ document service cluster if the selected graphics are included in the secret set.

23. (Currently amended) The method of claim 17 further comprising:

generating the private key portions for individuals registering, wherein the private key portions can be used with ~~signing identification~~ the service credentials to construct complete private keys;

associating the generated private key portions with the recorded identities of individuals registering; and

storing private key portions in a private key database.

24.-45. (Cancelled).